Accellion Share Securely™

AN ACCELLION WHITE PAPER

Best Practices for Secure Enterprise Content Mobility

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

WP-CM0312

Executive Summary

The proliferation of mobile devices and the popularity of Bring Your Own Device (BYOD) are creating new security challenges for enterprises. Employees are using consumer devices such as iPads and Android phones to access and store business data. To share this data, they're relying on email and consumer-class file-sharing services. As a result, data has never been easier to access and more difficult to secure. Security attacks against mobile devices are expected to increase in frequency and sophistication now that they're storing valuable data.

Enterprises need a data security solution for consumer mobile devices. Mobile Device Management (MDM) products provide a useful framework of provisioning mobile devices and enforcing basic security controls. But MDM solutions do not address the file-sharing and collaboration needs of mobile users.

To secure mobile devices while enabling employees to share data securely, enterprises need a comprehensive and flexible solution for Secure Enterprise Content Mobility. Complementing MDM products, the Secure Enterprise Content Mobility solution should ensure that mobile workers can easily share data with other authorized users, while also ensuring that data is always safe and IT operations always compliant.

An effective Mobile Content Management solution supports BYOD policies, enables authorized users to share files of any size securely, gives IT managers fine-grained access controls for files and devices, and helps enterprises ensure that their mobile communications comply with internal data security policies and industry regulations. Mobile security should be flexible enough to let IT managers define and enforce policies that vary by position, department, geography, and security level. By making file-sharing safe and convenient, Mobile Content Management enables road warriors to be as productive as possible on any device anywhere, anytime.

Mobile Security Threats

A recent survey found that enterprise IT teams were most concerned about the following types of security threats for mobile devices:

- *Loss or theft of a device carrying sensitive information: 64%*
- *A malware-infected device connecting to an internal network: 59%*
- *A malware-infected app being downloaded to a mobile device: 37%*
- *Data leak from user uploading confidential data to a mobile device: 36%*

A rise in the popularity of mobile devices corresponds with a rise in data breaches. For example, a study by Manhattan Research found that when doctors' use of smartphones rose by 9%, data breaches rose 32%.

Sources:
http://www.informationweek.com/news/mobility/business/229402912,
http://www.ama-assn.org/amednews/2011/12/19/bil21219.htm

The Tidal Wave of Mobile Computing Is Upon Us

The proliferation of mobile devices and the popularity of Bring Your Own Device (BYOD) are creating new security challenges for enterprises. Employees are buying their own mobile devices, bringing them to work, using them to access both personal data and business data. Applications are expected to work not just over the Web but over the air. When business data is readily accessible through mobile applications, employees copy the data and share it by copying, emailing, or synchronizing files. Data has never been easier to access and more difficult to secure.

The consumerization of IT is changing employee expectations of how and where they prefer to work. To appreciate the transformation that's under way, consider these statistics:

- 3 out of 5 workers say they no longer need to be in the office to be productive.
- 32% of workers globally use more than one mobile device during the course of a workday.
- 27% of mobile users use a tablet for work. [1]
- Apple iPhones and iPads and Google Android devices—all of them consumer devices—now make up over 70% of the mobile devices used by mobile workers.[2]
- Mobile workers are using smartphones for email, web conferencing, social media for work, accessing Office documents, and note-taking.
- In 2010, Web-based email usage declined 6%, while mobile email access rose 36%.[3]

By now, nearly 72% of U.S. enterprises have adopted BYOD policies, giving in to employee demands and allowing users to pick their own mobile devices. IT departments have little choice but to conform IT infrastructure to accommodate the various consumer-grade devices users are bringing to work.

Mobile security was challenging enough before. Even supporting hundreds or thousands of mobile workers on a single platform such as BlackBerry could be time-consuming and error-prone. Now IT departments are facing even greater difficulties as they scramble to implement data security and compliance controls for a growing number of devices and situations. Meanwhile, security threats and industry regulations aren't going away.

Security attacks against consumer mobile devices are expected to increase, now that these devices are storing and transmitting valuable business data. IBM expects the number of software exploits aimed at mobile devices to double this year.[4] Meanwhile, industry regulators will continue to scrutinize enterprise networks, even though 73% of CIOs believe their mobile IT infrastructures are not yet secure enough to pass an audit. (Gartner) (For more information about mobile security threats, see the sidebar.)

[1,3] http://www.gottabemobile.com/2011/08/15/mobile-workforce-trends-productivity-knows-no-bounds-infographic/

[2] ChangeWave Research, a division of 451 Research, quoted in "The battle for third place in the mobile enterprise," Chris Hazelton, 451 Research, November 2011.

[4] http://www.csoonline.com/article/691043/mobile-security-threats-are-heating-up

How should executives make sense of these changes and challenges? Let's examine the mobile security landscape, feature by feature, and then conclude with some best practices for deploying mobile security solutions for keeping mobile users safe and productive.

Mobile Policy Management: Details Still Matter

What mobile workers have in common is their mobility. What is different is everything else: their roles, responsibilities, geographies, and security clearances.

Mobile security solutions need to be detailed and flexible enough to let IT managers define and enforce policies that vary by position, department, geography, and security level. Policies should be able to restrict access to apps, files, and workspaces according to an employee's role in the organization. Enterprises need mobile security policies that are as specific as the policies governing employees working on desktop computers and other in-house systems.

Mobile Device Management: Useful but Not Sufficient

To help IT departments provision, manage, and secure their mobile devices, about a third of enterprises have deployed Mobile Device Management (MDM) solutions.[5] MDM enables IT organizations to provide over-the-air (OTA) updates of applications, configuration settings, and data to mobile devices, including smartphones and tablets. IT

Finally, as users work more frequently with video and graphics, files sizes are ballooning past the traditional 10 MB file-size limit imposed by email. Users need an easy way to share files of all sizes with colleagues. File synchronization, which users can configure in a browser with no official IT intervention, seems to be the answer managers can use MDM systems to control which mobile devices are granted access to internal resources. Should a mobile device be lost or stolen, IT managers can use MDM to erase the device remotely the next time it connects to the Internet. Leading MDM solutions include product offerings from BoxTone, Good Technology, and MobileIron.

MDM solutions provide a useful framework of provisioning mobile devices and mobile apps and for enforcing fundamental device-security controls. But MDM solutions do not address the file-sharing and collaboration needs of mobile users. Mobile workers need support for secure cross-boundary communication. They also need access to the context of files, so they can understand the full ramifications of the data they're working with.

Mobile users will be most productive if they can send and receive files of any type and size to authorized users inside and outside the organization. Whether they're on the road or in a conference room at headquarters, it's also helpful if they have as much context as possible about files. Examples of context include comments and threaded discussions about the files being worked on. Automatic notifications of changes also keep mobile users up to date about the status of important files.

[5] http://www.informationweek.com/news/mobility/business/229402912?pr

MDM provides basic app and data provisioning, but it does not provide the features needed for securely integrating flexible file-sharing practices in the field with existing file sync, storage and collaboration services provisioned in the office.

Security for Mobile Apps

One of the great things about mobile platforms such as Apple iOS and Google Android is all their custom applications or "apps." For just about every business and leisure activity—from filing expense reports to playing Texas Hold 'Em—you can say, "There's an app for that."

One of the biggest threats to enterprise data security is, yes, all those apps. There are literally hundreds of thousands of them, many from small software companies whose reputations are unknown. Many apps are excellent, but many are mediocre, and some are risky. In April 2011, Google had to remove 58 applications from the Google Android Marketplace after it was discovered that the apps contained rootkit malware. By then, the apps had been installed on over 260,000 devices. To ensure that the devices were safe, Google had to remotely wipe the devices clean, deleting all their data.

Since then, Google has tried to monitor the Android marketplace more carefully. Apple has been diligent about the way they screen apps all along. Nonetheless, the threat of malicious apps remains. Users must be careful about what they download. Malware could infect a mobile device, leak data from the device to hackers, infect systems on internal networks after a sync operation, and become a vector for a major internal malware attack.
Apps are too valuable to be avoided all together. But any effective mobile security solution must include tools for limiting access to apps and ensuring that, once installed, apps behave properly and pose no threat.

Putting It All Together: Secure Enterprise Content Mobility

Security for mobile apps, role- and department-specific security policies, file-sharing through secure workspaces, collaboration features that complement and extend MDM security—put all this together and you have Secure Enterprise Content Mobility.

Security Enterprise Content Mobility brings the rules-based access controls, data encryption services, and reporting logging associated with enterprise content management solutions to mobile devices. It gives authorized users access to the business data they need, anywhere, any time, and on any authorized device, including consumer devices such as iPhones and Android phones. Along with screening of devices and mobile apps, Enterprise Content Mobility provides an essential layer of security and control for enterprises with mobile users.

Best Practices for Secure Enterprise Content Mobility

To support Security Enterprise Content Mobility, enterprises should think in terms of devices, content, apps, and security. Here are some best practices for supporting Secure Enterprise Content Mobility:

Support More Devices

A Secure Enterprise Content Mobility solution should support whatever mix of mobile devices mobile users are carrying. In organizations that have adopted BYOD policies, Apple iPhones and Android phones are replacing BlackBerrys, but all three platforms remain popular. In the course of a typical day, many employees use multiple devices running different operating systems, so supporting a single user might involve supporting both BlackBerry and iOS, for example.

Support Better Content

When you're on the road, getting a file is useful, but getting a file and immediately understanding why it was revised and what sensitive issues it contains is invaluable. Secure workspaces that provide context for data, making it easy for mobile users to track discussions and revisions of important files. Providing context eliminates the need for perfunctory back-and-forth communications, such as long email threads about document revisions. When employees can quickly find and understand the data they need, they become more productive.

Employees are working with files that are larger than ever before: media files, graphics, medical images, etc. Users need to be able to share and discuss multi-gigabyte files, even if they're not downloading these files to every mobile device.

For organizations using enterprise content systems such as Microsoft SharePoint or Autonomy iManage, it only makes sense to integrate them with new services that support mobile users.

Extend Mobile Security

Deploy a Secure Enterprise Content Mobility solution with dashboards and logging features that give administrators complete visibility and control over file-sharing activities and mobile access policies. Administrators should be able to enforce detailed access controls for individual files and for shared workspaces, going beyond the typical app and data security controls of MDM solutions. Files should be encrypted both at rest and in transit. File owners and administrators should be able to set expiration dates for files, so sensitive data isn't left exposed on servers. A mobile content security solution should ensure that mobile access never jeopardizes data security or regulatory compliance.

Data on mobile devices needs to be secure, but mobile workers also need to be productive, communicating and collaborating with their co-workers and other peers. This often means exchanging sensitive data with partners, consultants, and even customers—users who are not likely to have accounts on an internal LDAP server. A mobile content security solution should support legitimate "cross-boundary" communication without turning mobile communications into a free-for-all.

Finally, the solution should include security and audit controls that support compliance with industry regulations such as GLBA, HIPAA, and SOX. Ease-of-use and employee productivity should never come at the expense of industry

regulations and federal and state laws. Enterprises need to stay compliant while making life easier for their mobile employees.

Conclusion

By following these best practices for Secure Enterprise Content Mobility, you'll give your mobile workers access to the critical business data they need, anywhere, any time, and on any authorized device, including tablets and smartphones. Enterprise Content Mobility provides an essential layer of security and control for mobile computing, ensuring that greater convenience and productivity never come at the expense of security.

About Accellion

The world's leading corporations and government enterprises rely on Accellion secure file sharing and collaboration solutions to secure their enterprise information and ensure compliance. Founded in 1999, Accellion, Inc. provides enterprise-class secure file sharing solutions that deliver the ease-of-use internal and external users need while giving the enterprise organization the protection it needs.

Accessible to employees and external users from the Web, iPad, iPhone, Android and Blackberry mobile devices, Accellion secure file sharing solutions offer the widest choice of deployment options spanning virtual and public, private, or hybrid cloud environments.

The company is headquartered in Palo Alto, California with offices in North America, Asia, and Europe. For more information please visit www.accellion.com or call (650)-485-4300. Follow Accellion's Blog, Twitter, Facebook, and LinkedIn.

For information about how Accellion delivers a Secure Enterprise Content Mobility Solution, please visit www.accellion.com.